IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR KING COUNTY

HEATHER LOSCHEN, individually and on behalf of all others similarly situated, Plaintiffs, v. SHORELINE COMMUNITY COLLEGE, an agency of the State of Washington, Defendant.	NO. **CLASS ACTION COMPLAINT**

Plaintiff Heather Loschen, by and through her counsel, individually and on behalf of all others similarly situated, alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Shoreline Community College ("SCC") is a Washington State community college that offers academic and professional degrees to about 8,000 students each year. SCC's goal is to be "recognized for inclusive excellence in teaching and learning, student success, and community engagement."[1]

2. To work or enroll at SCC, SCC requires individuals like Plaintiff to provide

[1] *See* Vision and Mission, https://www.shoreline.edu/about-shoreline/strategic-plan.aspx (las visited January 8, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

their SCC with confidential and sensitive information. As SCC stored and handled such highly-sensitive private information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

3. But while Plaintiff and others like her expected that SCC would keep that information safe and secure, SCC failed to implement and maintain adequate security protocols in storing and/or transferring this information, and as a result, hackers stole it.

4. Specifically, in February and March 2023, hackers gained access to SCC's computer systems and accessed the most sensitive private information of over 400,000 individuals. Ultimately, SCC failed to fulfill its obligations as unauthorized cybercriminals breached SCC's information systems and databases and stole vast quantities of private information belonging Plaintiff and Class members. This breach—and the successful exfiltration of Private Information—were direct, proximate, and foreseeable results of multiple failings on the part of SCC.

5. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of SCC's failure to reasonably safeguard Plaintiff's and Class members' private information, and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, and protection of their private information.

II. PARTIES

6. Plaintiff Heather Loschen is an individual and is a resident of King County, Washington. Plaintiff was an enrolled student at SCC in the Spring of 2023.

7. Defendant SCC is a Washington State agency located in Shoreline, King County, Washington.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

III. JURISDICTION AND VENUE

8. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010 and RCW 4.92.090.

9. This Court has personal jurisdiction over SCC because it is a Washington State agency and it is located in King County.

10. Venue is proper in this county pursuant to RCW 4.12.020(3) and RCW 4.92.010(1) because a substantial part of the events or omissions giving rise to these claims occurred in this county, and Plaintiff resides in King County, Washington.

III. FACTUAL BACKGROUND

11. SCC is a Washington State community college that offers academic and professional degrees to about 8,000 students each year.[2]

12. In order to enroll or work at SCC, Plaintiff and the Class Members were required to provide certain personal information to SCC. This information included, but was not limited to, an individual's full name, address, phone number, date of birth, Social Security number, individual taxpayer identification number (ITIN), citizenship status, and immigration status (collectively, "Private Information"). SCC informs prospective students that if they do not submit their Social Security number or ITIN, then they may be subject to civil penalties.[3] SCC also informs applicants that pursuant to state and federal law, the SCC will protect the applicant's Social Security number from unauthorized use and disclosure.[4]

13. SCC also collects and maintains certain personal information of its students through the storage and transmittal of the US Department of Education Federal Student Aid

[2] https://www.shoreline.edu/about-shoreline/ (last visited November 21, 2023)
[3] *Admission Application*, Shoreline Community College, https://www.shoreline.edu/apply-and-aid/registration/documents/application-for-admission.pdf (last visited November 21, 2023).
[4] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

information.

14. In 2022, the Federal Bureau of Investigation (FBI), in conjunction with other organizations, released a cybersecurity advisory alerting the public that it had recently observed institutions in the education sector had been frequent targets of ransomware attacks in recent years.[5] The advisory alerted that ransomware attacks may increase over the 2022/2023 school year, and the FBI encouraged organizations to implement certain mitigation efforts it recommended, including reviewing the security of third-party vendors; implementing policies for remote access that only allows systems to execute known and permitted programs; documenting and monitoring external remote connections; requiring all accounts with password logins to comply with National Institute Standards and Technology (NIST) password standards; and require phishing-resistant multifactor authentication for all services to the extent possible (particularly for webmail), among others.[6]

15. Notwithstanding the FBI's guidance, on March 20, 2023, SCC learned it had been the subject of a ransomware incident that affected the school's computer systems.[7] During the course of SCC's investigation, it discovered some of its data had been accessed by an unauthorized third party between February 27, 2023 and March 20, 2023.[8] On April 5, 2023 it confirmed data accessed by the unauthorized third party included the personal and confidential information of some students, staff, and faculty, including their names, social security numbers, passport numbers, driver's license numbers, dates of birth, financial account numbers, and/or

[5] *#StopRansomeware: Vice Society*, Cybersecurity Advisory, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0#main (last visited November 29, 2023).
[6] *Id.*
[7] *Notice of Data Breach*, Shoreline Community College, https://www.shoreline.edu/about-shoreline/notice-of-data-breach.aspx (last visited November 29, 2023).
[8] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

attestations regarding Covid-19 test results.[9]

16. After the ransomware incident, SCC officials advised students, staff, and faculty to watch out for suspicious or unauthorized activity in their accounts, to review credit reports and financial account statements, and to notify their financial institutions of fraudulent activity.[10] SCC provided complimentary memberships to a credit monitoring service to those who information was accessed.[11]

17. As a result of the ransomware attack, most students were forced to transition to remote work for a week, and Wi-Fi connections on campus were down.[12]

18. In total, SCC notified approximately 400,000 individuals, including current and former students, staff, and faculty of the cybersecurity attack that may have involved some of their Private Information.

Effects of the Data Breach on Plaintiff Heather Loschen

19. Plaintiff Loschen is a student of SCC and provided her private information to SCC as a condition of enrolling in classes at SCC.

20. Plaintiff Loschen reasonably understood and expected that SCC would safeguard her Private Information, and that it would timely and adequately notify her in the event that there was a data breach affecting her Private Information. Plaintiff would not have allowed SCC, or anyone in Defendant's position, to maintain or store her Private Information if she believed that SCC would not implement reasonable industry standards to safeguard her Private Information from unauthorized access.

---

[9] *Id.*
[10] *Shoreline Community College says personal info was accessed in attack*, The Seattle Times, https://www.seattletimes.com/seattle-news/shoreline-community-college-says-personal-info-was-accessed-in-attack/ (last visited November 29, 2023).
[11] *Id.*
[12] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

21. On April 14, 2023, SCC notified Plaintiff Loschen via email (a copy of which is attached as Exhibit A) that the cybersecurity incident described above may have involved her Private Information.[13] The email stated one of the following data elements of Plaintiff Loschen's may have been accessed: Social Security number, passport number, driver's license number, date of birth, financial account numbers, and/or attestation regarding COVID-19 test results.[14]

22. In the notice, SCC offered Plaintiff Loschen a complimentary membership in Experian Identity Works, a credit monitoring service.[15] SCC also warned Plaintiff to be vigilant for "signs of unauthorized activity by reviewing your credit reports and financial account statements."[16]

23. Plaintiff Loschen greatly values her privacy and her Private Information. She takes reasonable steps to maintain the confidentiality of her Private Information, including not opening links or emails she does not recognize.

24. Plaintiff Loschen stores any and all documents containing Private Information in a secure location. She also diligently chooses unique usernames and passwords for her various online accounts.

25. Plaintiff Loschen has made reasonable efforts to mitigate the impact of the data breach, including, but not limited to: researching the data breach, reviewing her financial account statements for any indications of actual or attempted identity theft or fraud, and researching credit monitoring and identity theft protection services offered by SCC.

26. Plaintiff Loschen has spent at least 7 hours dealing with the Data Breach to

[13] Exhibit A (Loschen Notice Email).
[14] *Id*.
[15] *Id*.
[16] *Id*.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

date, valuable time she otherwise would have spent on other activities, including, but not limited to, work, recreation, or time with family.

27. As a result of the data breach, Plaintiff Loschen has suffered emotional distress due to the release of her Private Information, which she believed SCC had protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her personal information for purposes of identity theft and fraud. Plaintiff Loschen remains very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

28. Plaintiff Loschen suffered actual injury from having her Private Information compromised as a result of the data breach, including but not limited to: (a) damage to and diminution in the value of her Private Information, a form of property that SCC obtained from Plaintiff Loschen; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

29. As a result of the data breach, Plaintiff Loschen anticipates spending considerable time and money on an ongoing basis to attempt to mitigate and address harms caused by the data breach.

30. As a result of the data breach, Plaintiff Loschen is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Effects of the Data Breach on the Class

31. Plaintiff Loschen's experience in connection with the data breach is typical of those of the Class Members.

32. Given the sensitive nature of the Private Information stolen in the data breach, hackers can commit identity theft, financial fraud, and other identity-related fraud against

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff and Class Members now and into the indefinite future.

33. As a result of the data breach, Plaintiff and Class Members will have to take a variety of steps to monitor for and safeguard against identity theft, and they are at a much greater risk of suffering such identity theft. In addition, these victims of the data breach are at a higher risk of potentially devastating financial identity theft. As the Bureau of Justice Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[17]

34. The Private Information exposed in SCC's data breach is highly coveted and valuable on underground or black markets. A cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web," exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Private Information to: (a) commit immigration fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) access financial accounts and records; or (f) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during arrest.

35. Consumers are injured every time their data is stolen and placed on the dark web. Each data breach victim is at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

36. The Private Information accessed in the Data Breach is also very valuable to SCC. SCC collects, retains, and uses this information as part of its enrollment process—without

[17] U.S. Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2012 (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf (last visited November 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

students enrolled, SCC would not receive their tuition payments. But SCC students value the privacy of this information, and they expect SCC to allocate enough resources to ensure it is adequately protected. Students would not have enrolled with SCC, provided their Private Information, and/or paid the same prices for SCC's services had they known SCC did not implement reasonable security measures to protect their Private Information. Students expect that the payments they make to their education institutions incorporate the costs to implement reasonable security measures to protect their Private Information.

37. The Private Information accessed in the Data Breach is also very valuable to Plaintiff and Class members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable Private Information to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class members' Private Information has been compromised and lost significant value.

38. Plaintiffs and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the Private Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Private Information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their Private Information and when they discover the harm. For

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

39. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

40. As the result of the data breach, Plaintiff and Class Members are likely to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

A. losing the inherent value of their personal information;

B. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

C. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

D. lowered credit scores resulting from credit inquiries following fraudulent activities;

E. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the data breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

annoyance of dealing with the repercussions of the data breach; and

F. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Private Information being in the possession of one or many unauthorized third parties.

41. If a consumer is lucky enough to be reimbursed for a financial loss due to identity theft or fraud, the consumer typically must expend significant time and effort to do so. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[18]

42. In addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose Private Information was accessed in the Data Breach, Plaintiff retains an interest in ensuring there are no future breaches. On information and belief, SCC is still in possession, custody, or control of Plaintiff's and the Class members' Private Information.

IV. CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action individually and behalf of a class (the "Class") preliminarily defined as:

> All individuals residing in the United States whose personal information was compromised in the data breach disclosed by SCC in April 2023.

44. Excluded from the Class are the following: SCC and SCC's officers and directors, and any judge to whom this case is assigned, as well as his or her staff and immediate family.

[18] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited 12/8/2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

45. Plaintiff reserves the right to amend the class definition.

46. This action satisfies the numerosity, commonality, typicality, and adequacy requirements of CR 23.

a) **Numerosity**. The proposed Class consists of at least 400,000 members—far too many to join in a single action.

b) **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, or control.

c) **Typicality**. Plaintiff's claims are typical of Class members' claims, as they arise from the same data breach, the same alleged negligence of and/or statutory violations by SCC, and the same unreasonable manner of notifying individuals regarding the data breach.

d) **Adequacy**. Plaintiff will fairly and adequately protect the interests of the proposed Class. Plaintiff's interests do not conflict with those of the Class. Plaintiff has retained counsel experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the Class, including in the capacity as lead counsel.

e) **Commonality.** Plaintiff and Class members' claims raise predominantly common factual and legal questions that can be answered for all Class members through a single class-wide proceeding. For example, to resolve any Class member's claims, it will be necessary to answer the following questions:

A. Whether SCC failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the personal information compromised in the data breach;

B. Whether SCC's conduct was negligent; and

C. Whether Plaintiff and Class are entitled to damages, attorney's fees, and/or

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

injunctive relief.

47. In addition to satisfying the prerequisites of CR 23(a), the action satisfies the requirements for maintaining a class action under CR 23(b). Common questions of law and fact predominate over any questions affecting only individual members, and a class action is superior to individual litigation or any other available methods for the fair and efficient adjudication of this action. In the alternative, class certification is appropriate because SCC has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the Class as a whole.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
Claim of Relief for Plaintiff and the Class Against Defendant SCC

48. Plaintiff re-alleges and incorporates by reference all paragraphs as though fully set forth herein.

49. SCC collected and stored Private Information from Plaintiff and the Class and had a corresponding duty to protect such information from unauthorized access.

50. SCC failed to inform Plaintiff and Class that its systems were inadequate to safeguard the Private Information they provided, and further failed to inform Plaintiff and the Class that providing personal information to SCC could lead to attackers gaining access to their Private Information.

51. The sensitive nature of the Private Information and economic value of it to hackers necessitated security practices and procedures sufficient to prevent unauthorized access to the Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

52. SCC failed to implement and maintain adequate security practices and procedures to prevent the data breach.

53. It was reasonably foreseeable to SCC that its failure to implement and maintain reasonable security procedures and practices would leave the Private Information in its systems vulnerable to breach and could thus expose the owners of that information to harm.

54. Further, given the known risk of major data breaches, and the increased risk of ransomware attacks on educational institutions, Plaintiff and the Class are part of a well-defined, foreseeable, finite, and discernable group that was at high risk of having their Private Information stolen.

55. SCC's duty to the Plaintiff and the Class arose out of its knowledge that individuals trusted it to protect their Private Information, especially given that SCC required that Private Information as a condition of student enrollment and/or employment at SCC. Only SCC was in a position to ensure that its own protocols were sufficient to protect against the harm to Plaintiff and the Class from a data breach of its own systems.

56. SCC knew, or should have known, of the vulnerabilities in its security practices and procedures, and the importance of adequate security to SCC students and staff and the owners of the Private Information.

57. Plaintiff and the Class have suffered harm as a result of SCC's negligence. These victims suffered diminished value of their Private Information. Plaintiff and the Class also lost control over the Private Information SCC exposed, which subjects each of them to a greatly enhanced risk of identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft, in addition to the time and expenses spent mitigating those injuries and preventing further injury.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

58. Consistent with RCW 4.92.100, Plaintiff Loschen, on her own behalf and on behalf of the Class she seeks to represent, presented a Tort Claim Form to the Washington Department of Enterprise Services' Office of Risk Management for the State's tortious conduct as set forth herein. More than sixty days have elapsed since she presented her claim, but SCC has not responded. *See* RCW 4.92.100.

IV. PRAYER FOR RELIEF

WHEREFORE, Plaintiff makes the following prayer for relief, individually and on behalf of the proposed Class:

A. An order certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiff and her counsel to represent the Class;

B. An order awarding Plaintiff and Class members monetary relief, including actual damages and penalties;

C. An order awarding injunctive relief requested by Plaintiff, including, but not limited to, an order:

i. Prohibiting SCC from engaging in the wrongful and unlawful acts described herein;

ii. Requiring SCC to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and state or local laws;

iii. Requiring SCC to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

iv. Prohibiting SCC from maintaining the Private Information of Plaintiff

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

and Class Members on a cloud-based database;

v. Requiring SCC to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SCC's systems on a periodic basis, and ordering SCC to promptly correct any problems or issues detected by such third-party security auditors;

vi. Requiring SCC to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. Requiring SCC to segment data by, among other things, creating firewalls and access controls so that if one area of SCC's network is compromised, hackers cannot gain access to other portions of SCC's network;

viii. Requiring SCC to establish an information security training program that includes at least annual information security training for all students and staff, with additional training to be provided as appropriate based upon the individuals' respective responsibilities with handling personal information, as well as protecting the Private Information of Plaintiff and Class Members;

ix. Requiring SCC to routinely and continually conduct internal training and education, and, on an annual basis, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

x. Requiring SCC to meaningfully educate all Class Members about the threats that they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xi. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a COS 2 Type 2 attestation on an annual basis to evaluate SCC's compliance with the terms of the Court's final judgment, to provide such report the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. An award of costs of suit an attorneys' fees, as allowed by law;

E. An award of pre-judgment and post-judgment interest, as provided by law;

F. Leave to amend this Complaint to conform to the evidence produced at trial; and

G. Such other and further relief as this Court may deem just and proper.

Dated: January 8, 2024

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Kaleigh N. Boyd*

Kaleigh N. Boyd, WSBA #52684
kboyd@tousley.com
Joan M. Pradhan, WSBA #58134
jpradhan@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
Tel: 206.682.5600
Fax: 206.682.2992